

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**

In Re Application of:

Simpson, et al.

Group Art Unit: 2137

Serial No.: 10/029,960

Examiner: Pyzocha, Michael

Filed: December 21, 2001

Docket No. 10007659-1

For: **Document Notarization System and Method**

**APPEAL BRIEF IN RESPONSE TO NOTIFICATION OF  
NON-COMPLIANT APPEAL BRIEF**

Mail Stop: Appeal Brief-Patents  
Commissioner for Patents  
P.O. Box 1450  
Alexandria, Virginia 22313-1450

Sir:

The Notice of Non-Compliant Appeal Brief mailed August 13, 2007 has been carefully considered. Applicant submits this Appeal Brief in response.

It is not believed that extensions of time or fees are required to consider this Appeal Brief. However, in the event that additional extensions of time are necessary to allow consideration of this paper, such extensions are hereby petitioned under 37 C.F.R. § 1.136(a), and any fees required therefor are hereby authorized to be charged to Deposit Account No. 08-2025.

### **I. Real Party in Interest**

The real party in interest is Hewlett-Packard Development Company, LP, a limited partnership established under the laws of the State of Texas and having a principal place of business at 20555 S.H. 249 Houston, TX 77070, U.S.A. (hereinafter "HPDC"). HPDC is a Texas limited partnership and is a wholly-owned affiliate of Hewlett-Packard Company, a Delaware Corporation, headquartered in Palo Alto, CA. The general or managing partner of HPDC is HPQ Holdings, LLC.

### **II. Related Appeals and Interferences**

There are no known related appeals or interferences that will affect or be affected by a decision in this Appeal.

### **III. Status of Claims**

Claims 2-4, 14-16 have been canceled leaving claims 1, 5-13, and 17-31 stand finally rejected. No claims have been allowed. The final rejections of claims 1, 5-13, and 17-31 are appealed.

### **IV. Status of Amendments**

This application was originally filed on December 21, 2001, with twenty-three (23) claims. In a Response filed October 26, 2005, Applicant amended claims 1, 5-7, 9, 10, 12, 13, 21, canceled claims 2-4 and 14-16, and added new

claims 24-31. In a Response filed January 19, 2006, Applicant amended claims 17, 18, and 24.

All of the above-identified amendments have been entered and no other amendments have been made to any of claims 1, 5-13, and 17-31. The claims in the attached Claims Appendix (see below) reflect the present state of those claims.

## **V. Summary of Claimed Subject Matter**

The claimed inventions are summarized below with reference numerals and references to the written description ("specification") and drawings. The subject matter described in the following appears in the original disclosure at least where indicated, and may further appear in other places within the original disclosure.

Independent claim 1 describes a method for notarizing imaging data. The method comprises retrieving imaging data on behalf of a user via a network from the user's personal imaging repository with a network-based notarization service via an imaging extension. *Applicant's specification*, page 24, line 17 to page 25, line 3; Figure 8A, item 802.

The method of claim 1 further comprises electronically notarizing the imaging data with the network-based notarization service. *Applicant's specification*, page 6, lines 1-3; Figure 8B, item 812.

Independent claim 13 describes a network-based notarization system for notarizing imaging data. The system comprises means (308, 310, Fig. 3; 418,

Fig. 4) for retrieving imaging data on behalf of a user via a network from the user's personal imaging repository via an imaging extension. *Applicant's specification*, page 24, line 17 to page 25, line 3; Figure 8A, item 802.

The system of claim 13 further comprises means (316, Fig. 3; 414, Fig. 4) for electronically notarizing the imaging data. *Applicant's specification*, page 6, lines 1-3; Figure 8B, item 812.

Independent claim 21 describes a network-based notarization service stored on computer-readable media. The service comprises logic (308, 310, Fig. 3; 418, Fig. 4) configured to retrieve a document on behalf of a user via an imaging extension, the document being stored in a personal imaging repository of the user. *Applicant's specification*, page 24, line 17 to page 25, line 3; Figure 8A, item 802.

The service of claim 21 further comprises logic (316, Fig. 3; 414, Fig. 4) configured to electronically notarize the document. *Applicant's specification*, page 6, lines 1-3; Figure 8B, item 812.

## **VI. Grounds of Rejection to be Reviewed on Appeal**

The following grounds of rejection are to be reviewed on appeal:

1. Claims 1, 5-13, 17-23, and 29-31 have been rejected under 35 U.S.C. § 102(e) as being anticipated by *Epstein* (U.S. Pat. No. 6,601,172).
2. Claims 24 and 25 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Epstein* as applied to claims 1 and 5, respectively, in view of *Schrieber, et al.* ("Schreiber," U.S. Pat. No. 6,298,446).
3. Claims 26 and 27 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Epstein* as applied to claim 6, in view of *Braam, et al.* ("Braam," U.S. Pat. No. 6,957,347).
4. Claim 28 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Epstein* as applied to claim 7, in view of *Natarajan* (U.S. Pat. No. 6,611,599).

## **VII. Arguments**

The Appellant respectfully submits that Applicant's claims are neither anticipated under 35 U.S.C. § 102 nor obvious under 35 U.S.C. § 103, and respectfully requests that the Board of Patent Appeals overturn the final rejections of those claims at least for the reasons discussed below.

### **A. Claim Rejections - 35 U.S.C. § 102(e)**

Claims 1, 5-13, 17-23, and 29-31 have been rejected under 35 U.S.C. § 102(e) as being anticipated by *Epstein* (U.S. Pat. No. 6,601,172). Applicant respectfully traverses this rejection.

It is axiomatic that "[a]nticipation requires the disclosure in a single prior art reference of each element of the claim under consideration." *W. L. Gore & Associates, Inc. v. Garlock, Inc.*, 721 F.2d 1540, 1554, 220 USPQ 303, 313 (Fed. Cir. 1983). Therefore, every claimed feature of the claimed invention must be represented in the applied reference to constitute a proper rejection under 35 U.S.C. § 102(e).

In the present case, not every feature of the claimed invention is represented in the Epstein reference. Applicant discusses the Epstein reference and Applicant's claims in the following.

#### **1. The Epstein Disclosure**

Epstein discloses transmitting revisions with digital signatures. *Epstein*, Patent Title. Included in Epstein's invention is electronic notarizing. The notarizing

process is described in relation to Figures 1a-1d. As described by Epstein, an author creates a report on a workstation. *Epstein*, column 2, lines 33-37. The author's workstation hashes the report and encrypts the hash using the author's private key to form a signature for the report. *Epstein*, column 2, lines 40-48. The workstation then transmits the report and the signature to a customer's server. *Epstein*, column 2, lines 55-57. The server hashes the report and decrypts the author's signature using the author's public key. *Epstein*, column 2, lines 60-62.

The server then sends *the author's signature* to a notary's host system. *Epstein*, column 3, lines 6-9. The notary host system receives *the author's signature*, creates a time stamp containing the author's signature, receipt time, notary id, sequence number, and customer id. *Epstein*, column 3, lines 15-17. The notary host system hashes the time stamp and signs it using the notary's private key, and then returns to the server the time stamp and the notary's signature. *Epstein*, column 3, lines 17-22. The server stores the time stamp and the notary's signature "*with relation to the report.*" *Epstein*, column 3, lines 28-32 (emphasis added).

As can be appreciated from the above, Epstein's notary host system does *not* retrieve image data to be notarized. Moreover, Epstein's notary host system does *not* notarize such image data. Instead, Epstein's notary host system notarizes *an author's signature* that is sent to the notary host system from a customer server that received imaging data (a "report") from an author's workstation.

## **2. Applicant's Claims**

Epstein fails to teach several of Applicant's claim limitations. Applicant discusses some of those claim limitations in the following.

### **a. Claims 1, 5-12, and 29-31**

Applicant's claim 1 provides as follows (emphasis added):

1. A method for notarizing imaging data, comprising:  
*retrieving imaging data on behalf of a user* via a network  
*from the user's personal imaging repository* with a network-based  
notarization service *via an imaging extension*; and  
*electronically notarizing the imaging data* with the network-  
based notarization service.

#### **(i) Network-Based Notarization Service "Retrieving Imaging Data on Behalf of a User"**

As a first matter, Epstein does not teach a "network-based notarization service" "retrieving imaging data on behalf of a user". As is noted above, an author's workstation *transmits* a report and a signature to a customer's server. Later, the server then *sends* the author's signature to a notary's host system. Therefore, no "notarization service" in Epstein's system retrieves "imaging data" on behalf of a user for the purpose of notarizing. Instead, imaging data (i.e., the report) is sent to a customer server and only a signature is sent from the customer server to a notary host system.



Applicant further notes that the above-discussed limitation is not, as was argued by the Examiner, taught in column 4, lines 19-22 of the Epstein reference. That portion of Epstein's disclosure provides as follows:

In a first group of steps 160 in FIG. 2a, *the author* creates an image and transfers the image to a server which signs the image for the author and stores the image.

*Epstein*, column 4, lines 19-22 (emphasis added).

The above expert explicitly states that the *author* "transfers" the image to the customer server. It is not stated that the server "retrieves the image" on the author's behalf. Moreover, the "server" identified in the excerpt is not the "notary host system" that performs notarization on the author's signature.

Regarding column 5, lines 15-47, also identified by the Examiner, that portion of the Epstein disclosure provides as follows:

In the final set of steps 210 in FIG. 2d, a user requests the image for viewing on a viewer and the stored image is provided along with the two time stamps and the two notary's signatures so that the viewer can verify the origin and certification date of the original image and the origin and certification date of the revision and that according to the server the revision is a product of the original image. In step 212, the user requests the image using the viewer. The viewer may be any equipment that allows the image to be played to the user. The viewer is not restricted to visual display and may be, for example, a loud speaker playing an audio image. In step 213, the server sends the image hash, the imager id, the image condensation, both related time stamps (one for the image and one for the compressed image)

and similarly both notary's signatures to the viewer. In step 214, the viewer hashes the condensation time stamp and decrypts the notary's signature for the condensation using the notary's public key in order to verify the digital time and other information in the condensation time stamp. In step 215, the viewer hashes the image time stamp and decrypts the notary's image signature using the notary's public key to verify the image time stamp. In step 216, the viewer hashes the condensation, and in step 217, the viewer combines the condensation hash and the notary's image signature and decrypts the servers's condensation signature to verify the condensation time stamp including the condensation time. In step 218, the viewer combines the image hash and the imager id and decrypts the server's image signature to verify the imager id and imaging time. In step 219, the viewer compares the image time stamp time and the condensation time stamp time to verify that the times are very close. In step 220, viewer displays the image, imager id, imaging time and condensing time to the user.

*Epstein*, column 5, lines 15-47.

Clearly, the above excerpt does not disclose "retrieving imaging data on behalf of a user . . . with a network-based notarization service". Although the excerpt can be interpreted as generally describing retrieving image data *for the user* to view, retrieval is not performed by a "network-based notarization service". Instead, it is the user that is retrieving his data. Applicant acknowledges that it is known for a user to retrieve his data to view it. What is not known and not taught by Epstein, however, is a network-based notarization service retrieving the data on behalf of the user.

**(ii) "From the User's Personal Imaging Repository"**

Second, Epstein does not teach that such retrieval is "from the user's personal imaging repository". As is stated above, Epstein does not teach a notarization service "retrieving" imaging data at all. Moreover, Epstein is silent as to the concept of a "personal imaging repository". Again, a proper rejection under 35 U.S.C. § 102 requires that a reference teach *each and every limitation* of a rejected claim.

**(iii) "Retrieving . . . Via an Imaging Extension"**

Third, Epstein does not teach that retrieval of imaging data from the user's personal imaging repository is accomplished via an "imaging extension". Once again, Epstein does not even contemplate retrieval by a notarization service of imaging data or a personal imaging repository. Furthermore, Epstein says absolutely nothing about an "imaging extension". As is described in Applicant's specification, an "imaging extension" is a component that is called upon to act as a gateway to access the user's personal imaging repository. Applicant's specification, page 9, line 11 to page 10, line 24. The term should be interpreted consistent with that definition. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 34 USPQ2d 1321 (Fed. Cir. 1995)(in banc), *aff'd*, 517 U.S. 370, 38 USPQ2d 1461 (1996) ("Claims must be read in view of the specification, of which they are a part").

In the Advisory Action, the Examiner argues that Epstein teaches an "imaging extension" in column 5, lines 15-47, which is reproduced above.

However, a review of that excerpt proves that Epstein provides no such teaching. In particular, no component is described in that excerpt that functions for a network-based notarization service to retrieve imaging data on behalf of a user from the user's personal imaging repository. Epstein's "viewer" is merely a program that is used by the user to display images. It is not used to retrieve imaging data for a network-based notarization service. Indeed, because it is the author who is viewing the image, no such "imaging extension" is necessary. In other words, the author already knows the location of the image and already has authorization to access to it. Applicant refers back to page 9, line 11 to page 10, line 24 of Applicant's specification for a detailed discussion of what the claimed imaging extension is and what functions it serves.

#### (iv) "Notarizing the Imaging Data"

Fourth, Epstein does not teach "electronically notarizing the imaging data". As is described above, Epstein does not teach notarizing the author's "report." Instead, as is described above, a customer server that receives the author's report and the author's signature *sends only the author's signature to a notary's host system*. As a result, the notary host system does not notarize the author's report at all. Instead, the notary host system returns only a time stamp and the notary's signature to the server, which then stores the time stamp and the notary's signature *"with relation to the report."* *Epstein*, column 3, lines 28-32 (emphasis added).

Applicant further notes that column 4, lines 19-22 of the Epstein reference, reproduced above, do not, as suggested by the Examiner, teach notarizing imaging

data. Specifically, the action of the customer server *signing* the image does not equate to *notarizing* the image. We know this because, later in column 4 with further reference to the method of Figure 2a, Epstein states that the server "establishes a connection with the notary's host, and in step 173, the server sends the server's image signature to the host". *Epstein*, column 4, lines 43-45. Therefore, the server's signing the image is a step performed *prior* to the notarization that is performed on the *server's signature* and not the image itself by the separate notary host system.

#### **(v) Dependent Claims**

From the above, it is clear that claim 1 is allowable over Epstein. Given that claims 5-12, 29, and 31 incorporate the limitations of claim 1, these claims are allowable over Epstein for at least the same reasons. Applicant notes, however, that many of the dependent claims contain further limitations that are not taught by Epstein.

Regarding dependent claim 5, Epstein does not teach that the imaging extension comprises "part of a user browser". Even if Epstein's "viewer" were interpreted to comprise an "imaging extension", *nowhere* does Epstein state that the viewer comprises part of a user browser.

Regarding dependent claim 6, Epstein does not teach that the imaging extension comprises "part of the network-based notarization service". In particular, if Epstein's viewer is interpreted to comprise an "imaging extension", the viewer clearly does not form part of Epstein's "notary host system."

Regarding dependent claim 7, Epstein does not teach that "notarizing" comprises "modifying the imaging data by adding at least one of a stamp and a digital signature to the imaging data". Although the user in the Epstein system signs the "report," Epstein's notary host system creates a time stamp and signs *the time stamp*, not the report itself. See *Epstein*, column 3, lines 17-22.

Regarding dependent claim 8, Epstein does not teach a notarization service "modifying" imaging data (i.e., the report). It follows then the Epstein does not teach "storing the modified imaging data".

Regarding dependent claim 9, Epstein does not teach a "personal imaging repository" as discussed above.

Regarding dependent claims 10-12, Epstein does not teach the concept of a "notarization certificate". Instead, as described above, Epstein's notary host system only hashes a time stamp and signs it using the notary's private key, and then returns to the server the time stamp and the notary's signature. See *Epstein*, column 3, lines 17-22.

Regarding dependent claim 31, Epstein does not teach a notarization server that "internally stores" the notarization. Again, Epstein's notary host system is only described as returning its signed time stamp to the "customer server." See *Epstein*, column 3, lines 17-22. Epstein does not, however, state that the host notary system stores anything.

**b. Claims 13 and 17-20**

Applicant's claim 13 provides as follows (emphasis added):

13. A network-based notarization system for notarizing imaging data, comprising:

*means for retrieving imaging data on behalf of a user via a network from the user's personal imaging repository via an imaging extension; and*

*means for electronically notarizing the imaging data.*

Regarding claim 13, Epstein fails to teach "means for retrieving imaging data . . . via a network from the user's personal imaging repository via an imaging extension" or "means for electronically notarizing the imaging data", at least for reasons discussed in relation to claim 1. For those reasons, Applicant submits that claims 13 and 17-20 are allowable over Epstein.

The claims that depend from claim 13 contain further limitations not taught by Epstein. For example, regarding dependent claim 17, Epstein does not teach an imaging extension that comprises "part of a user browser". See discussion of claim 5 above.

Regarding dependent claim 18, Epstein does not teach an imaging extension that comprises "part of the network-based notarization service." See discussion of claim 6 above.

Regarding dependent claim 19, Epstein does not teach that the means for "notarizing" comprises "means for modifying the imaging data by adding at least

one of a stamp and a digital signature to the imaging data". See discussion of claim 7 above.

Regarding dependent claim 20, Epstein does not teach the concept of a "notarization certificate". See discussion of claim 10 above.

**c. Claims 21-23**

Applicant's claim 21 provides as follows (emphasis added):

21. A network-based notarization service stored on computer-readable media, comprising:

*logic configured to retrieve a document on behalf of a user via an imaging extension, the document being stored in a personal imaging repository of the user; and*

*logic configured to electronically notarize the document.*

Regarding claim 21, Epstein fails to teach "logic configured to retrieve a document . . . via an imaging extension, the document being stored in a personal imaging repository of the user" or "logic configured to electronically notarize the document", at least for reasons discussed in relation to claim 1. For those reasons, Applicant submits that claims 21-23 are allowable over Epstein.

The claims that depend from claim 21 contain further limitations not taught by Epstein. For example, regarding dependent claim 22, Epstein does not teach that the logic configured to "notarize" comprises "logic configured to modify the imaging data by adding at least one of a stamp and a digital signature to the imaging data". See discussion of claim 7 above.



Regarding dependent claim 23, Epstein does not teach the concept of a "notarization certificate". See discussion of claim 10 above.

### **C. Conclusion**

Due to the shortcomings of the Epstein reference described in the foregoing, Applicant respectfully asserts that Epstein does not anticipate Applicant's claims. Therefore, Applicant respectfully requests that the rejection of these claims be withdrawn.

### **B. Claim Rejections - 35 U.S.C. § 103(a)**

As has been acknowledged by the Court of Appeals for the Federal Circuit, the U.S. Patent and Trademark Office ("USPTO") has the burden under section 103 to establish a *prima facie* case of obviousness by showing some objective teaching in the prior art or generally available knowledge of one of ordinary skill in the art that would lead that individual to the claimed invention. See *In re Fine*, 837 F.2d 1071, 1074, 5 U.S.P.Q. 2d 1596, 1598 (Fed. Cir. 1988). The Manual of Patent Examining Procedure (MPEP) section 2143 discusses the requirements of a *prima facie* case for obviousness. That section provides as follows:

To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art

reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in applicant's disclosure.

In the present case, the prior art does not teach or suggest all of the claim limitations, and there is no suggestion or motivation in the prior art to modify the references to include those limitations.

#### **1. Rejection of Claims 24 and 25**

Claims 24 and 25 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Epstein* as applied to claims 1 and 5, respectively, in view of *Schrieber, et al.* ("Schreiber," U.S. Pat. No. 6,298,446). Applicant respectfully traverses this rejection.

As is identified above, Epstein does not teach several aspects of Applicant's claims. In that Schreiber does not remedy the deficiencies of the Epstein reference, Applicant respectfully submits that claims 24 and 25 are allowable over the Epstein/Schreiber combination for at least the same reasons that claim 1 is allowable over Epstein.

With particular regard to the limitations of claim 24, Epstein's "viewer," which is relied upon by the Examiner as comprising an "imaging extension", is not described as comprising an API. Applicant notes that, there is no legitimate motivation provided by the prior art to modify that viewer to comprise an API. Moreover, Schrieber does not, as argued by the Examiner, teach such an imaging

extension in column 18, lines 19-38. That portion of the Schreiber reference provides as follows:

In a preferred embodiment, the present invention prevents a user from using Windows API functions, such as BitBlt, StretchBlt, PlgBlt, GetPixel and GDI32, to copy protected image data, by including software within the user's web browser that substitutes other functions for those Windows API functions. For example, the software within the user's web browser provides a substitute BitBlt function, which is invoked instead of the standard system BitBlt function when the user issues a command to copy data from the video display buffer. The substitute BitBlt function includes special logic for dealing with protected image data, but is otherwise identical to the standard system BitBlt function. The special logic serves to supply substitute pixel data instead of protected image data, so that the data that is copied to the user's clipboard is different from the raw pixel data of protected images. For example, the special logic can compose watermarks and/or a text message onto protected image pixel data, or it can encrypt protected image pixel data, or it can supply a completely white image instead of a protected image.

*Schreiber*, column 18, lines 19-38.

As is clear from that excerpt, Schreiber is describing APIs that are used to "copy protected image data" from web sites, *not* retrieve imaging data on the behalf of a user from the user's personal imaging repository. Therefore, Schreiber's APIs are not "imaging extensions" that perform the functions stated in Applicant's claims.

Regarding claim 25, Schreiber clearly does not describe any "generic access instructions" that call upon an "imaging extension" to "access the user's

personal imaging repository". Simply stated, Schreiber contemplates nothing of the sort.

## **2. Rejection of Claims 26 and 27**

Claims 26 and 27 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Epstein* as applied to claim 6, in view of *Braam, et al.* ("*Braam*," U.S. Pat. No. 6,957,347). Applicant respectfully traverses this rejection.

As is identified above, Epstein does not teach several aspects of Applicant's claims. In that Braam does not remedy the deficiencies of the Epstein reference, Applicant respectfully submits that claims 26 and 27 are allowable over the Epstein/Braam combination for at least the same reasons that claim 1 is allowable over Epstein.

With particular regard to the limitations of claim 26, Epstein does not contemplate use of a browser to view the user's images or a user directly accessing a network-based notarization service. It follows that there would be no motivation to provide the capability of determining a location of the user's personal imaging repository from a "redirection address used to visit the network-based notarization service".

Regarding claim 27, Epstein does not contemplate any "authentication procedure" or using a browser to access a notarization service. It follows that there is no motivation to add performance of an authentication procedure "performed by the user by visiting a network-based authentication service".

### **3. Rejection of Claim 28**

Claim 28 has been rejected under 35 U.S.C. § 103(a) as being unpatentable over *Epstein* as applied to claim 7, in view of *Natarajan* (U.S. Pat. No. 6,611,599). Applicant respectfully traverses this rejection.

As is identified above, Epstein does not teach several aspects of Applicant's claims. In that Braam does not remedy the deficiencies of the Epstein reference, Applicant respectfully submits that claim 28 is allowable over the Epstein/Natarajan combination for at least the same reasons that claim 1 is allowable over Epstein.

With particular regard to the limitations of claim 28, Epstein does not contemplate modifying imaging data at all. Instead, "notarization" is provided in the form of a time stamp that is signed by Epstein's notary host system. Therefore, there is no legitimate motivation to place a "watermark" on Epstein's report. Again, Epstein's notary host system does not even receive the report in the first place.

### **VIII. Conclusion**

In summary, it is Applicant's position that Applicant's claims are patentable over the applied prior art references and that the rejection of these claims should be withdrawn. Appellant therefore respectfully requests that the Board of Appeals overturn the Examiner's rejection and allow Applicant's pending claims.

Respectfully submitted,

By: 

David R. Risley

Registration No. 39,345

**Claims Appendix under 37 C.F.R. § 41.37(c)(1)(viii)**

The following are the claims that are involved in this Appeal.

1. A method for notarizing imaging data, comprising:

retrieving imaging data on behalf of a user via a network from the user's personal imaging repository with a network-based notarization service via an imaging extension; and

electronically notarizing the imaging data with the network-based notarization service.

- 2-4. (Canceled)

5. The method of claim 1, wherein the imaging extension comprises part of a user browser.

6. The method of claim 1, wherein the imaging extension comprises part of the network-based notarization service.

7. The method of claim 1, wherein electronically notarizing imaging data comprises modifying the imaging data by adding at least one of a stamp and a digital signature to the imaging data.

8. (Original) The method of claim 7, further comprising storing the modified imaging data.

9. The method of claim 8, wherein the modified imaging data are stored in the user's personal imaging repository.

10. The method of claim 1, wherein electronically notarizing imaging data comprises generating a notarization certificate.

11. (Original) The method of claim 10, further comprising storing the notarization certificate.

12. The method of claim 11, wherein the notarization certificate is stored in the user's personal imaging repository.



13. A network-based notarization system for notarizing imaging data, comprising:

means for retrieving imaging data on behalf of a user via a network from the user's personal imaging repository via an imaging extension; and

means for electronically notarizing the imaging data.

14-16. (Canceled)

17. The system of claim 13, wherein the imaging extension comprises part of a user browser.

18. The system of claim 13, wherein the imaging extension comprises part of the network-based notarization service.

19. (Original) The system of claim 13, wherein the means for electronically notarizing imaging data comprise means for modifying the imaging data by adding at least one of a stamp and a digital signature to the imaging data.

20. (Original) The system of claim 13, wherein the means for electronically notarizing imaging data comprise means for generating a notarization certificate.

21. A network-based notarization service stored on computer-readable media, comprising:

logic configured to retrieve a document on behalf of a user via an imaging extension, the document being stored in a personal imaging repository of the user; and

logic configured to electronically notarize the document.

22. (Original) The service of claim 21, wherein the logic configured to electronically notarize the document comprises logic configured to modify the document by adding at least one of a stamp and a digital signature to the document.

23. (Original) The service of claim 21, wherein the logic configured to electronically notarize the document comprises logic configured to generate a notarization certificate.

24. The method of claim 1, wherein the imaging extension comprises application programming instructions (API).

25. The method of claim 5, wherein content is downloaded from the network-based notarization service to the user browser, the content comprising generic access instructions that call upon the imaging extension to access the user's personal imaging repository.

26. The method of claim 6, wherein the network-based notarization service determines the location of the user's personal imaging repository from a redirection address used to visit the network-based notarization service, the redirection address comprising information identifying the location of the user's personal imaging repository.

27. The method of claim 26, wherein the redirection address is generated upon successful completion of an authentication procedure performed by the user by visiting a network-based authentication service.

28. The method of claim 7, wherein the stamp comprises a watermark that is applied to a document that comprises the imaging data.

29. The method of claim 7, wherein the digital signature comprises the identity of the network-based notarization service that notarized the imaging data and the date the notarization occurred.

30. The method of claim 10, wherein the notarization certificate comprises the identity of the network-based notarization service that notarized the imaging data and the date the notarization occurred.

31. The method of claim 1, wherein the notarization is internally stored by the network-based notarization service that performed the notarization.

**Evidence Appendix under 37 C.F.R. § 41.37(c)(1)(ix)**

There is no extrinsic evidence to be considered in this Appeal. Therefore, no evidence is presented in this Appendix.

**Related Proceedings Appendix under 37 C.F.R. § 41.37(c)(1)(x)**

There are no related proceedings to be considered in this Appeal.

Therefore, no such proceedings are identified in this Appendix.